## **Confidentiality**

1. Confidential Information: information in whatever form (including in written, oral, visual or electronic form or on any magnetic or optical disk or memory) and wherever located relating to Grace Christian Academy's business, students, teachers, teaching assistants, customers, suppliers, products, assets, affairs and finances that is confidential to us and trade secrets relating to our business or any of our suppliers, clients, customers, agents, shareholders, industry affiliates, sponsors, donors, management or business contacts, including technical data and know-how that you create, develop, receive or obtain in connection with the your Employment whether or not such information (if in anything other than oral form) is marked confidential.

The Employee acknowledges that during the ordinary course of his or her employment, he or she will have access to and/or may be exposed to Confidential Information including, technology, processes, products, plans, financial or other information or data of Employer and that of the Employer’s suppliers, clients, stakeholders, students, employees and customers, which may amount to a trade secret, be confidential or commercially sensitive and, which, if misused or disclosed, could cause significant harm to the Employer.

Such information, whether communicated in writing, electronically or in any other medium (and whether or not it is marked as confidential), is referred to as “confidential information” and shall in particular include (without limitation) the following:

1. the Employer’s intellectual property rights;
2. details of how the Employer or any stakeholder prices its products or services including any discounts, incentives or non-standard terms offered to any client;
3. information relating to the Employer’s suppliers, prices, salaries, clients, stakeholders, students, employees and customers and the terms and conditions (including any prices, incentives, and discounts) agreed upon with them;
4. research and development projects of the Employer and/or any stakeholder;
5. the Employer’s or stakeholder’s marketing and sales strategies and plans;
6. potential acquisitions and disposals by the Employer;
7. the Employer’s financial and academic performance;
8. any processes, inventions, designs, know-how, discoveries, technical specifications, and other technical information relating to the creation, production, or supply of any past, present, or future product or service of the Employer; and
9. any other categories of confidential information that the Employer wants to protect and of which it notifies the employee in writing as being confidential, or which by its nature or the surrounding circumstances is clearly confidential.

It is understood that confidential information shall not be shared by the Employee with any unauthorized person, firm, company or organization outside of the Employer, or within the Employer except with clearly appropriate and authorized officials, either during or after termination of employment. In such cases where confidential information can be shared, it shall be done solely for the benefit of the Employer and not the individual, even if that information was developed or compiled by the individual during the time of employment.

Without prejudice to your common law duties, you shall not (except in the proper course of your duties, as authorised or required by law or as authorised by the Board either during your Employment or at any time after its termination (however arising):

* + 1. use any Confidential Information for your own benefit or for the benefit of any other person, company or other organisation whatever;
    2. make or use any Copies; or
    3. disclose any Confidential Information

**Copies**: means copies or records of any Confidential Information in whatever form (including in written, oral, visual or electronic form or on any magnetic or optical disk or memory) and wherever located, and any extracts, analysis, studies, plans, compilations or any other way of representing or recording and recalling information which contains, reflects or is derived or generated from Confidential Information.

The Employee shall be responsible for protecting confidential information and shall observe the following rules;

1. use his or her best efforts to prevent the use, disclosure or communication of any confidential information by any person, company or organisation (except in the proper course of your duties, as required by law or as authorised by the Principal or the Board); and
2. inform the Principal immediately upon becoming aware of, or suspecting, that any such person, firm or company or organisation knows or has used any confidential information.

The restrictions contained in this clause do not apply to the following:

1. any use or disclosure authorised by the Principal or required in the ordinary and proper course of the employee’s duties or as required by the order of a court of competent jurisdiction, or an appropriate regulatory authority, or otherwise required by obligation of law; or
2. any information that the employee can demonstrate was known to him or her prior to his or her employment with the Employer; or
3. any information that is already in, or comes into, the public domain other than through the employee’s unauthorised disclosure or breach of confidence, or
4. any information being deemed a protected disclosure by the employee within the meaning of section 2 of the Whistleblower Protection Act, 2015 (Revised).

The Employee will not, other than with the prior written approval of the Principal, make or issue any press, radio or television statement, or publish or submit for publication any letter or article, or post any content on any social media platform relating directly or indirectly to the business affairs of Grace Christian Academy or any of its students or staff members (whether current or past).

The provisions of this clause are without prejudice to the duties and obligations of the Employee which exist at common law or in equity.

The provision of this clause shall survive any termination of an employment contract and shall remain in force in relation to any item of confidential information for so long as it is still properly regarded by the Employer as being confidential.

All Confidential Information and Copies shall be our property and on termination of the Appointment, or the Board's request at any time during the Appointment, you shall:

* + 1. hand over all Confidential Information or Copies to the Principal;
    2. irretrievably delete any Confidential Information (including any Copies) stored on any magnetic or optical disk or memory, including personal computer networks, personal e-mail accounts or personal accounts on websites, and all matter derived from such sources which is in your possession or under your control outside our premises; and
    3. provide a signed statement that you have complied fully with your obligations under this Contract of Employment.

## **Data Protection**

The Employer understands its responsibilities with respect to data protection and supports the rights of all those whom it has a relationship with, including but not limited to, staff, students, parents and guardians of students, guests, and alumni. Grace Christian Academy is committed to:

* fully complying with all data privacy legislation;
* adhering to good practice as issued by appropriate bodies; and
* handling personal data with care and consideration recognizing the importance of such information.
  1. Grace Christian Academy will collect and process information relating to you in accordance with the Privacy Notice which is on the Website. You are required to sign and date a copy of the Privacy notice and return it to the School Secretary.
  2. You shall comply with the Data Protection Policy when handling personal data in the course of employment including personal data relating to any employee, worker, contractor, customer, client, supplier or agent of ours. You will also comply with our IT and communications systems policy.
  3. Failure to comply with the Data Protection Policy or any of the policies listed in clause     may be dealt with under our Disciplinary procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

The Employer has appointed a Data Protection Officer (the “**DPO**”) to monitor and advise on compliance with the Data Protection Act 2021 (Revised) and its accompanying regulations and guidance.

The Employer is committed to ensuring its staff have the necessary training and awareness in relation to data protection.

Information security is very important to the Employer and as such, in the event of a data protection incident (such as loss or theft of data and or equipment, ineffective controls allowing unauthorized access, equipment failure, accidental or unauthorized disclosure, human error or hacking) the **DPO must immediately be made aware.** The DPO will investigate and decide whether the incident constitutes a data protection breach.

It is necessary for the Employer to control and process personal data, sensitive or otherwise, for legal, personnel, administrative and management purposes, and in order to comply with all applicable laws and regulations and to fulfil Grace’s obligations as an employer, including, but not limited to the following areas:

1. controlling and processing information about the Employee’s physical or mental health or condition in order to monitor sick leave, entitlement to benefits and make decisions about the Employee’s fitness to work;
2. administering employment with the Employer, such as in the administration of the Employer’s human resources systems, payroll, pension scheme and benefit plans; and
3. complying with legal requirements and obligations to third parties, including insurance companies and, when required, providing information relating to any criminal proceedings in which the Employee may have been involved.

The Employer may make such information available to those who provide products or services to or for human resource and recruitment purposes (such as advisers and payroll administrators), regulatory authorities or any business unit within which the Employee works, and as may be required by law.

The Employee consents to the Employer transferring and storing data, including the Employee’s personal data to countries outside of the Cayman Islands, which may not have the data protection laws in place that are of similar standard to those in place in the Cayman Islands.

The Employee specifically and freely accepts that the Employer may take, or cause to be taken, a photograph of his or her likeness, and publish it on an internal company intranet and other internal media, and in some cases on our website or other externally published media or documents for the purpose of identification.

## **Monitoring**

The Employer’s electronic communication systems are not private or confidential and the Employee expressly consents to the Employer’s monitoring, recording, and intercepting any use that the Employee makes of the electronic communication systems operated or provided by the Employer for purposes including, but not limited to, the following;

1. to ensure, from time to time, that the policies and procedures of the Employer are being complied with;
2. for legitimate business purposes;
3. for preventing and detecting crime;
4. to investigate or detect the unauthorised use of the Employer’s computer systems;
5. to establish the existence of facts; and
6. to ascertain or demonstrate the standards which are achieved or ought to be achieved by Employees using the electronic communication system in the course of their duties.

The Employee shall comply with any electronic communication systems policies that the Employer may issue from time to time.